Network Visualization Tool (NVT)

Technical Interchange Meeting #5

November 1998

Ronda Henning

Kevin Fox

EXHIBIT 1A

HARRIS
Electronic Systems

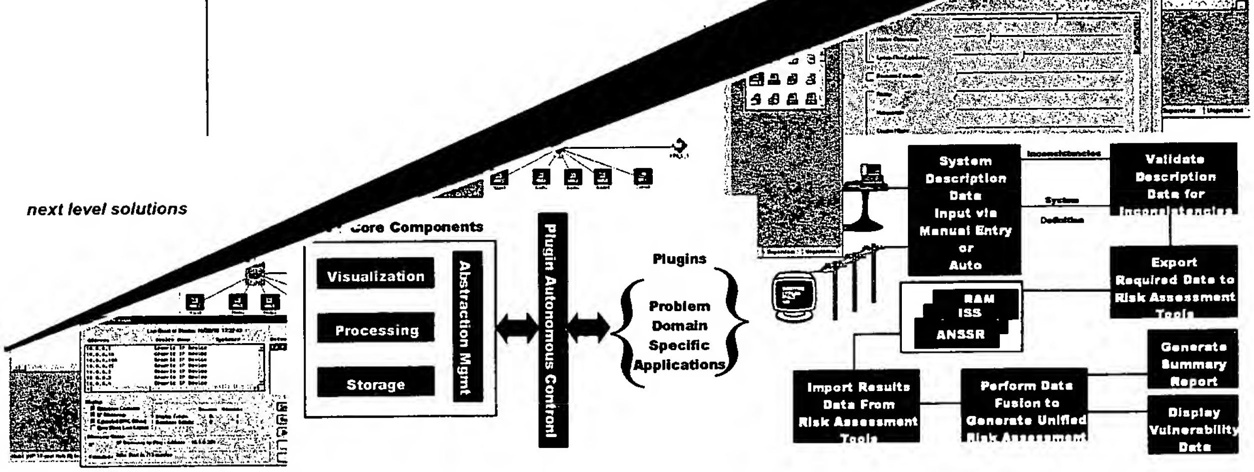
Network Visualization Tool (NVT) Program

Technical Interchange Meeting #5

November 1998

Ronda Henning
Kevin Fox

next level solutions



Introduction

Agenda

HARRIS Electronic Systems

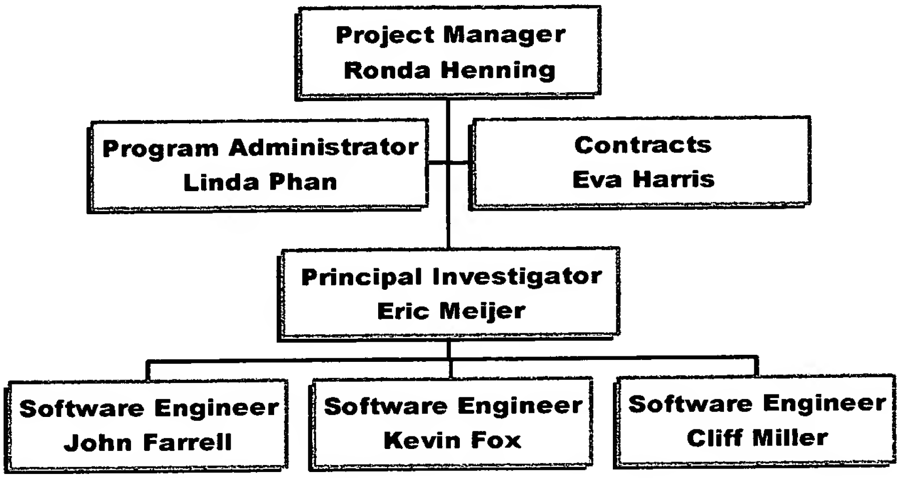
- •Introduction
- •Program Overview
- •NVT Architecture
- •Technology Assessment to Integrate Risk Tools
- •FuzzyCLIPS
- •Task #6 Proof-of-Concept Prototype
- •Future: Risk/Vulnerability Visualization
- •Plans for the Next Quarter
- •Open Discussion

Program Overview

Program Objective

- **To investigate technologies for the enhancement of automated risk assessment tools in the areas of usability, productivity and capability**
- **In particular, investigate enhancement through**
  - *New methods to perform knowledge solicitation*
  - *A normalized system representation satisfying the needs of several existing risk assessment tools*
  - *The fusion of various tool outputs into a single report*
  - *The graphical display of the resulting vulnerability data*

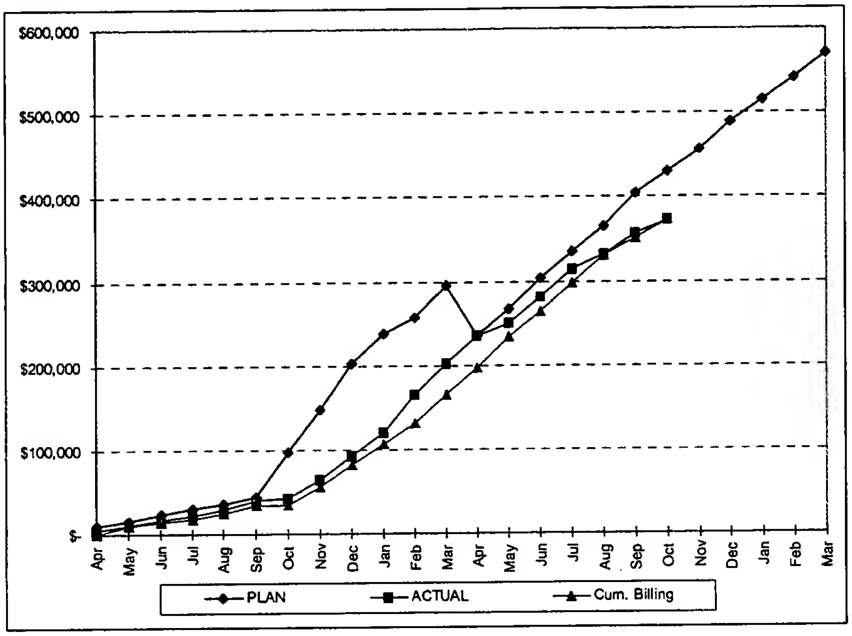
NVT Program Team



Financial Summary

HARRIS Electronic Systems

•Expenditures



Planned: $430.2K
Actuals: $372.6K

Expenditures/Staffing

HARRIS Electronic Systems

- **Program underrunning projections**
  - *–Planned underrun, to allow us to support new staff*
  - *–Addition of John Farrell full time 1 December*
    - •Expertise in Fuzzy CLIPS and G2
    - •Lots of incremental build/prototyping experience
  - *–Changes in contracts and finance staffing --*
    - •Benign, uncomplicated program for new staff
- **State of current incremental funding:**
  - *–Current authorized funding of $490,000*
  - *–Out of money in January*
  - *–$83,000 of planned incremental funding in GFY 1999 for contract completion.*

Program Schedule

HARRIS Electronic Systems

- Contract began 1 April 1997
- 24 month schedule, divided into 7 tasks
  - *Task #1 - Knowledge Solicitation*
  - *Task #2 - System Visualization and Validation*
  - *Task #3 - Selection and Application of Automated Reasoning Technologies (Risk Assessment Tools)*
  - *Task #4 - Vulnerability Quantification*
  - *Task #5 - Scaling of Indentified Vulnerabilities*
  - *Task #6 - Proof-of-Concept Prototype*
  - *Task #7 - Final Report*

HARRIS Electronic Systems

Insert Here NVT Schedule
from MS Project

Insert Here NVT Schedule
from MS Project

Current Status

HARRIS Electronic Systems

- **Task #1 - Completed**
  - *Resulted in selection of OpenView as discovery technology*
  - *Also have NET VIZ in NVT Lab*
- **Task #2 - On-going**
- **Task #3 - Completed**
  - *Resulted in selection of ANSSR, ISS, and RAM*
- **Task #4 - Vulnerability Quantification**
- **Task #5 - Underway**
  - *Resulted in selection of Fuzzy Expert System technology to integrate results from risk assessment tools*
- **Task #6 - Underway**
  - *Currently addressing issues with ANSSR*
- **Task #7 - Final Report**

NVT Architecture

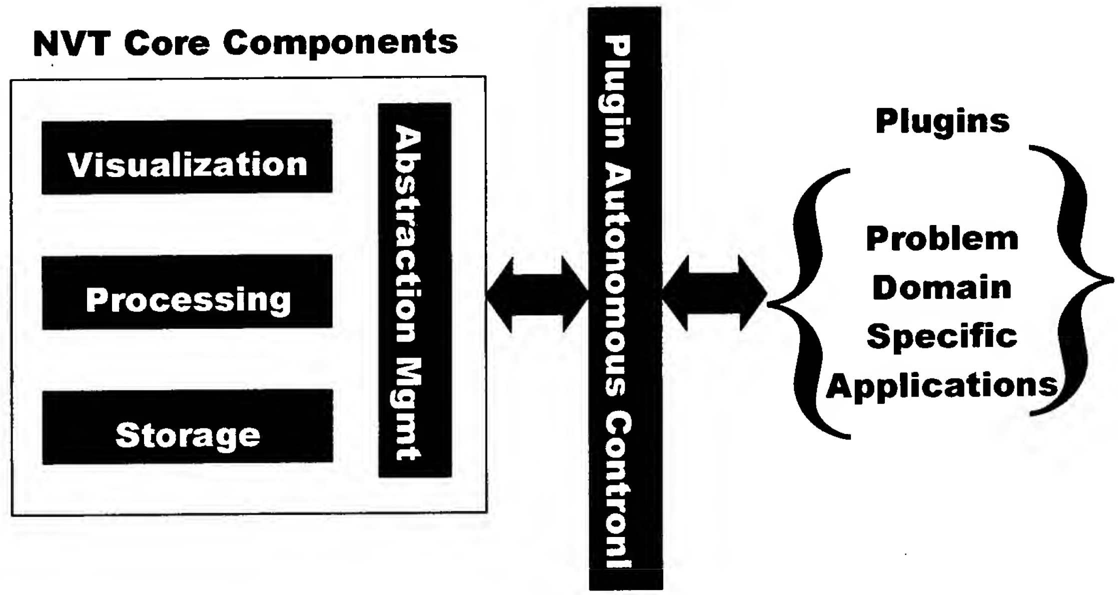
NVT Architecture Goals

HARRIS Electronic Systems

- Establish a framework that allows for the use of current and future risk assessment *plugins*
- Establish the foundation for a system that can resolve Ontological and Language issues
- Provide the user with a clear understanding of their present risk based on the most effective use of the current *plugin* set
- Provide the user with the capability to determine the most effective means to mitigate their risk

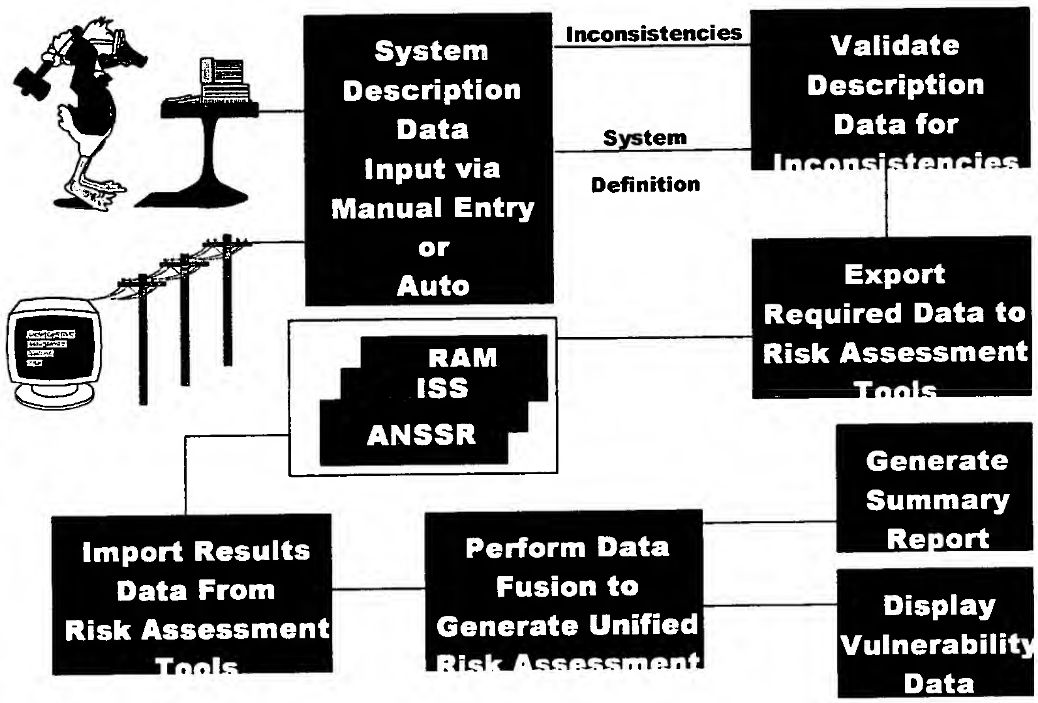
NVT Architecture Concept

HARRIS Electronic Systems



Analysis Flow Diagram

HARRIS Electronic Systems



Technology Assessment to Support Integration of Multiple Risk Assessment Tools

Technology Assessment

HARRIS Electronic Systems

- Assessed technology to implement a framework to support automated integration of multiple risk assessment tool outputs
- Focused on technologies that could best support our goal of integrating the products of multiple commercial applications into a common framework
- Examined a variety of products that exist in the market place today, including the inputs and outputs those products require

Technology Assessment

HARRIS Electronic Systems

- Analyzed a variety of technologies including:
  - *–Expert Systems*
  - *–Database Systems*
  - *–Neural Network/learning*
  - *–Fuzzy Logic*

Expert Systems

- Characterized by the developer's ability to model an expert in the technology for the particular problem domain
- Our framework is not focused on any particular problem domain
  - *Intent is to establish a generalized capability to allow a variety of tools to cooperatively work together*
  - *Specific problems within our framework may require an expert system*
  - *However, overall architecture did not fit the expert system profile*

Database Systems

HARRIS
Electronic Systems

- A collection of bits
- Provides a very rich capability for viewing those bits and establishing relationships between bits
- Problem is the user must have an understanding of the proper way to query the database
- With a variety of interdependent tools, the issue is not where are the bits, but what the bits mean
- Storage of bits will be isolated and normalized, but it is clear that the foundation for the framework cannot be a database system
  - *Foundation for our framework is the ability to categorize bits, establish relationships, and ask the right questions*
  - *The formulation of the right question (query) is beyond the scope of a traditional database*

Neural Network/Learning Systems

HARRIS Electronic Systems

- **Provide a technological foundation for learning**
  - *Learn in a modelless environment from relationships of data*
- **The problem with application to NVT is the lack of any real training sets (underlying relationships)**
  - *We do not know ahead of time, and therefore cannot teach, what the correct answer may be*
  - *Correct answer is also dependent on a variety of dynamic data sources that comes from the interaction of the system with itself and the real world*
  - *Without the ability to categorize the response to a given set of inputs, learning technologies do not provide the solution to our problem*

Neural Network/Learning Systems

HARRIS Electronic Systems

- However, some components of our framework may benefit from the ability to learn
- As the foundation continues to evolve it may be possible for the system to predict, based on past experience, the most applicable tool sets
- This predictive capability, however, is beyond our current goal of establishing the framework itself

Fuzzy Logic Systems

HARRIS Electronic Systems

- **Difficulty with many of other technologies is the assumption that a single, or very few, experts or cases can resolve problems presented to the system**
  - *In the real world, probability that a variety of experts will be in close agreement is very low*
  - *As the system complexity increases, this probability reduces significantly*
- **Another aspect of fuzzy systems that is different is the partitioning of the solution space**
  - *Typically in most systems, the solution is an evaluation of information into true or false statements*
  - *However, real world information is rarely an issue of true or false, but is in fact a generalization or degree of truth*

Fuzzy Logic Systems

HARRIS Electronic Systems

- Composed of rules, however, the rules do not need to be precise
  - *Can be changed by the system itself*
- Purpose of the rules is not to make a decision per rule
  - *Instead, it is to accumulate evidence for, or against, a set of probable solutions*
- Fuzzy rules are evaluated in parallel to provide an accumulated confidence for a particular outcome

Fuzzy Logic Systems

HARRIS Electronic Systems

- **An indication that fuzzy technology is applicable can be determined by evaluating the problem space itself**
  - *If the problem has a high degree of natural complexity or a self-referential architecture, this is indicative of a fuzzy type problem*
  - *The ability of fuzzy models to handle uncertainty and possibilities much better than conventional models is a significant benefit to us*
- **Another indicator of a fuzzy type problem is if the model will undergo regular revisions**
- **Fuzzy systems have a much higher degree of robustness and fault tolerance**

Fuzzy Logic Systems

- Provide a high level of flexibility and knowledge representation that can handle the significant ambiguities that are inherent in our architecture
- Work well, conceptually, within NVT because of their ability to provide a robust and predictable response in the presence of imprecise information
- Given the scope of the problem being addressed, it is clear that in many instances we will have a wide range of imprecision
  - *One of our goals is to allow the framework to minimize the imprecision by the application of knowledge extracted from the tools and fed back into the system itself*
- Also have the ability to explain their behavior, which in our risk assessment framework is critical

Fuzzy Technologies

- **Within fuzzy technology, several different areas were examined**
  - *–Fuzzy SQL*
  - *–Knowledge Mining*
  - *–Fuzzy Cognitive Maps*
  - *–Fuzzy Expert Technology*

Fuzzy Expert Technology

HARRIS
Electronic Systems

- Based on the premise that multi-criteria, multi-expert decision making can lead to a best-fit answer
- Primary benefit is its ability to use, and assimilate, knowledge from a variety of sources
- For NVT
  - *Expect to have both conflicting and collaborating experts*
    - Must be able to combine those opinions
  - *Need ability to support a set of independent fuzzy models rather than continuing to create a more complex set of rules for a single expert*
  - *Also need to carefully manage our rule space or the system will become impossible to update within a short period of time*

Fuzzy Expert Technology

HARRIS Electronic Systems

- **This technology is applicable because:**
  - *–An expert exists for each tool planned for inclusion in the system*
  - *–The problem itself is fuzzy, in that it has ambiguities and must deal with partial information*
  - *–We can incrementally learn and apply new technologies as the system grows*
  - *–We believe we can identify valid membership functions for the mapping of data to concept and concept to knowledge*
- **An upcoming activity is to identify concepts and their valid membership functions**

HARRIS Electronic Systems

An Introduction to FuzzyCLIPS

Cliff Miller

CLIPS & FuzzyCLIPS

HARRIS Electronic Systems

•What is CLIPS?

- *–Expert System Tool*
- *–Developed by Software Technology Branch, NASA*
- *–LISP-like syntax*
- *–C language*

•What is FuzzyCLIPS?

- *–An extension of CLIPS*
- *–Provides a mechanism to incorporate Fuzzy constructs into the expert system*

CLIPS & FuzzyCLIPS

HARRIS Electronic Systems

•Elements of CLIPS and FuzzyCLIPS

- *–CLIPS Shell (provides inferencing capabilities)*
- *– Functions, variables, commands, etc.*
- *– OOP Support*

•CLIPS Shell

–Fact-list:	*Global Memory for data*
–Knowledge Base:	*Rule base (contains rules)*
–Inference Engine:	*Controls overall execution of rules*

CLIPS - Facts & Rules

HARRIS Electronic Systems

- **Facts**
  - *May be asserted at run-time or pre-defined and initialized*
    - (sky blue)
    - (node 17 RESPONDING)

- **Rules**
  - *Rules may incorporate heuristic knowledge or experience*
  - *Rules follow the familiar IF-THEN construct, except they are fired by the inference engine based on pattern matching*
  - *Rule activation results from a new matching pattern entity or if an existing pattern entity is retracted and reasserted*
  - *If necessary, rule salience may be explicitly declared*

•Using Rules

```
(defrule my_rule_name "Optional comment"
        (pattern_1)
        (pattern_2 list_item another_list_item)
        (pattern_n)
=>
        (assert (some action)
        (assert (n number of actions)))

(defrule comfort_zone
        (temperature 73)
=>
        (printout t "We're comfortable!!!))
```

CLIPS - Variables

•**Variables**

–*Variables can be pattern matched, manipulated, and reasserted as new facts:*

```
(defrule get-solution-strength
        (cleaner-volume ?cleaner-oz)
        (water-volume ?water-oz)
=>
        (assert (solution-strength (/ ?cleaner-oz (+ ?cleaner-oz
        ?water-oz))))
```

deftemplate Contruct

HARRIS Electronic Systems

- **A deftemplate is similar to a record or a structure in some other programming languages.**

```
(deftemplate cleaning_solution "optional comment"
   (slot product
      (allowed-symbols WINDEX AMMONIA FANTASTIC)
      (default WINDEX))
   (slot concentration
      (type FLOAT)
      (default 0.50))
   (multislot used-for
      (type symbol)
      (default ?DERIVE)))

(assert (cleaning_solution (product WINDEX) (used_for
   windows glass)))
```

Procedural Constructs

HARRIS Electronic Systems

- **If Then**

```
(if (= ?x 0)
        then
        (printout t "zero" crlf)
        else
        (printout t "non-zero" crlf))
```

- **While**

```
(while (> ?x 0)
        (printout t ?x " bottles of beer on the wall" crlf)
        (bind ?x (- ?x 1)))
```

- **Functions**
  - *May be provided by CLIPS or user defined via deffunction*
  - *External functions written in another language may be called*
- **deffunction**

```
(deffunction <function-name> [optional comment]
   (?arg1 ?arg2 ...?argM [$?argN])  ;argument list.  Last one may
   (<action1>)                      ;be optional multifield arg.
   (<action2>)                      ;action1 to
     ...                            ;action(K-1) do not
   (<action(K-1)>)                  ;return a value
   (<actionK>)                      ;only last action returned
```

Example - NIM

HARRIS Electronic Systems

```
(reset)
(defrule move
  ?old_turn <- (myturn)
  ?old_count <- (count ?cur_count)
=>
  (retract ?old_turn)
  (retract ?old_count)
  (bind ?modval (mod (- ?cur_count 1) 4))
  ( if (= ?cur_count 1) then
    (printout t "Take: 1  Total: 0  I lose" crlf)
  else
    (if (= ?modval 0) then
      (bind ?play (+ 1 (mod (random) 3)))
    else
      (bind ?play ?modval))
    (assert (count (- ?cur_count ?play)))
    (printout t "Take: " ?play "  Total: " (-
     ?cur_count ?play) crlf)
    (assert (yourturn))))
(defrule start
  (initial-fact)
=>
  (printout t "Total: 23" crlf)
  (assert (count 23))
  (assert (yourturn)))

(defrule human
  ?old_turn <- (yourturn)
  ?old_count <- (count ?cur_count)
=>
  (retract ?old_turn)
  (retract ?old_count)
  (bind ?play (read))
  ( if (= 23 (- ?cur_count ?play)) then
    (assert (count ?cur_count))
    (assert (myturn))
  else
    (if (< ?play 4) then
      (if (= ?play ?cur_count) then
        (printout t "Take: 1  Total: 0  I win" crlf)
      else
        (assert (count (- ?cur_count ?play)))
        (printout t "Take: " ?play "  Total: " (-
   ?cur_count ?play) crlf)
        (assert (myturn)))
    else
      (assert (count ?cur_count))
      (assert (yourturn)))))
```

- **CLIPS Object Oriented Language (COOL)**
  - *Provides standard OOP constructs including:*
    - abstraction
    - encapsulation
    - inheritance
    - polymorphism

CLIPS Classes

HARRIS Electronic Systems

- All classes are children of one or more super-class
- Inheritance by specialization (e.g. horse is-a mammal) is directly supported.
- Multiple inheritance is supported
- Some handlers (known as methods in some other OOLs) are predefined under the CLIPS provided USER class; other handlers are user defined
- Handlers are invoked by sending messages to objects

```
(defclass CLEANING_SUPPLY (is-a USER) (role abstract)
   (slot condition (create-accessor read-write) (default CLEAN)))
(defclass SCRUBBRUSH (is-a CLEANING_SUPPLY) (role concrete)
   (slot bristle_length (create-accessor read-write)))
(make-instance Bobs_brush of SCRUBBRUSH
(bristle_length 1)
   (condition DIRTY))
(send [Bobs_brush] get-bristle_length)
1
(send [Bobs_brush] get-condition)
DIRTY
(defmessage-handler CLEANING_SUPPLY wash ()
   (dynamic-put condition CLEAN))
(send [Bobs_brush] wash)
(send [Bobs_brush] get-condition)
CLEAN
```

FuzzyCLIPS

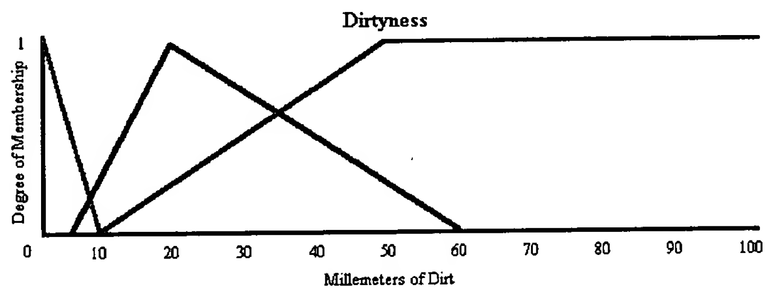
HARRIS Electronic Systems

- An extension of standard CLIPS that allows for the use of fuzzy facts and fuzzy rules which contain both membership functions and certainty factors
- Provides an expanded syntax for the representation of facts and rules
- Provides commands and features to facilitate working with fuzzy sets

FuzzyCLIPS Concepts

HARRIS Electronic Systems

- The world often does not fit into discreet "all or nothing" categories
- Fuzzy logic relies upon the degree of truth of a given statement, or the degree of membership within a set
- An expert often uses vague rules with inexact hedges
  - *"If the window is SLIGHTHLY dirty, use a LITTLE Windex"*
  - *A fuzzy expert system can handle such rules well*



•Certainty Factors

–Degree of certainty of facts or rules is easily expressed in FUZZYClips

((assert (floor very dirty)) CF 0.8)

•Membership functions

–FuzzyCLIPS membership functions may be defined using:

- •A set of discrete singleton points (this can represent triangular membership functions, trapezoidal membership functions, or any other function that may be represented or approximated by a set of line segments)
- •One of three predefined standard curves
- •Linguistic expressions

FuzzyCLIPS Examples

HARRIS Electronic Systems

```
(deftemplate fz_dirtyness
    0 100 mm ; lower and upper bounds, units (millimeters of dirt)
    ((clean (0 1) (10 0))
    (getting_grungy (5 0) (20 1) (60 0))
    (filthy (10 0) (50 1))))

(deftemplate surface
    (slot type (type SYMBOL))
    (slot dirtyness (type FUZZY-VALUE fz_dirtyness)))

(assert (surface (type window) (dirtyness getting_grungy)) CF 0.8)
(assert (surface (type floor) (dirtyness (50 0) (52 1) (55 0))) CF 0.9)

(defrule clean_grungy_window
    (declare (CF 0.7))
    (surface (type window) (dirtyness getting_grungy))
=>
```

Want More Information ?

HARRIS Electronic Systems

- CLIPS
  - *http://www.ghg.net/clips/CLIPS.html*
- FuzzyCLIPS
  - *http://ai.iit.nrc.ca/fuzzy/fuzzy.html*

Task #6
Proof-of-Concept Prototype

Task #6

HARRIS Electronic Systems

- **The integration of three distinct risk analysis/ vulnerability analysis reasoning engines into a proof-of-concept prototype of the Network Vulnerability Visualization Architecture, currently known as the Network Visualization Tool (NVT)**

- **Activities**
  - *Acquire FuzzyCLIPS & Develop Simple Examples*
    - Obtain the latest version of the FuzzyCLIPS development environment
    - Have the team become familiar and/or re-acquainted with the tool through the development of some simple examples that we can possibly apply to later phases of the program

Task #6 Activities

HARRIS
Electronic Systems

- Acquire/Study Vulnerability Assessment Tools
  - *Obtain the three vulnerability tools selected*
  - *One tool was chosen to represent each of the different categories of vulnerability tools*
    - ANSSR was selected as a prime example of a legacy reasoning engine
    - ISS Internet Scanner was selected as an example of a "live" vulnerability tool
    - RAM was selected because of our experience using it for large scale, highly complex problems such as the power distribution system and because it was selected for the Secret and Below Initiative (SABI)
  - *Once in-house, learn the tools requirements for input/output/reasoning, to determine the most appropriate way to create individual tool "plug-ins"*

Task #6 Activities

HARRIS
Electronic Systems

- Design Initial Prototype
  - *Using the preliminary architecture currently in place, translate this high-level design to a much more concrete, cohesive design that can be "built-to"*
  - *This involves the laying out of the NVT design to a per-functional module level, so the team can do incremental prototyping and we can track levels of completion*

Task #6 Activities

HARRIS Electronic Systems

•Decide Test Scenario/System

- *–NVT is supposed to execute against any network topology*
- *–What we need to use for testing purposes is a few sample networks*
- *–These can be segments of the Harris network, the AFRL network, or a C3I system net such as CTAPS or GTN*
- *–The ideal would be to work with a network that the customer can identify with, and use for his own subsequent demonstration purposes*

Task #6 Activities

HARRIS Electronic Systems

- **Acquire Basic System Information (for Demo Team)**
  - *When the candidate demonstration application has been selected, obtain the network data*
  - *For example, a "canned" ping/discovery session, a live discovery session, or a sit down and draw the network session*

Task #6 Activities

- Complete Graphical User Interface (GUI)
  - *Determine the GUI, do not invent new visualization techniques, but focus on applying work already done in other related areas, such as data fusion, message understanding, virtual reality, etc.*
  - *Understand that this probably at least a two part GUI, one for input and one for output.*

Task #6 Activities

HARRIS Electronic Systems

- **Develop Fuzzy Knowledge Expert for 3 Risk Tools**
  - *Fuzzy Expert works on multiple levels, or layers of data manipulation*
    - For example, there is one level, that of output combination to result in a meaningful, close to plain English output result
    - There is another layer, that looks for missing information related to data ingest operations, where a single tool may not have all the information, but another tool might have a way to compensate
    - Also, there may be layers for criticality or relevance of data as well for each tool
    - The question is how to most effectively address the various layers with some degree of cohesion while preserving system modularity and maintainability

Task #6 Activities

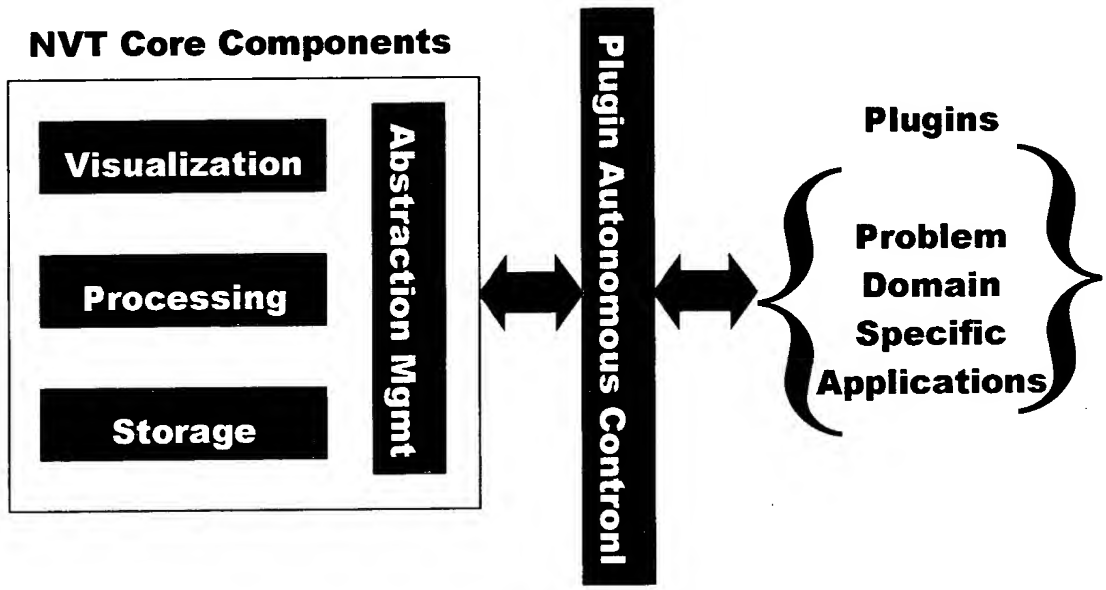
HARRIS Electronic Systems

- **Integration and Test (in Melbourne)**
  - *The final integration/demonstration testing, that determines removal and/or documentation of the problems*
- **Ship Equipment to AFRL/RRS**
  - *Pack it all up, and send it out*
- **Deliver, Demonstrate and Test (in Rome)**
  - *Take it to Rome and make it happen for final sell-off*

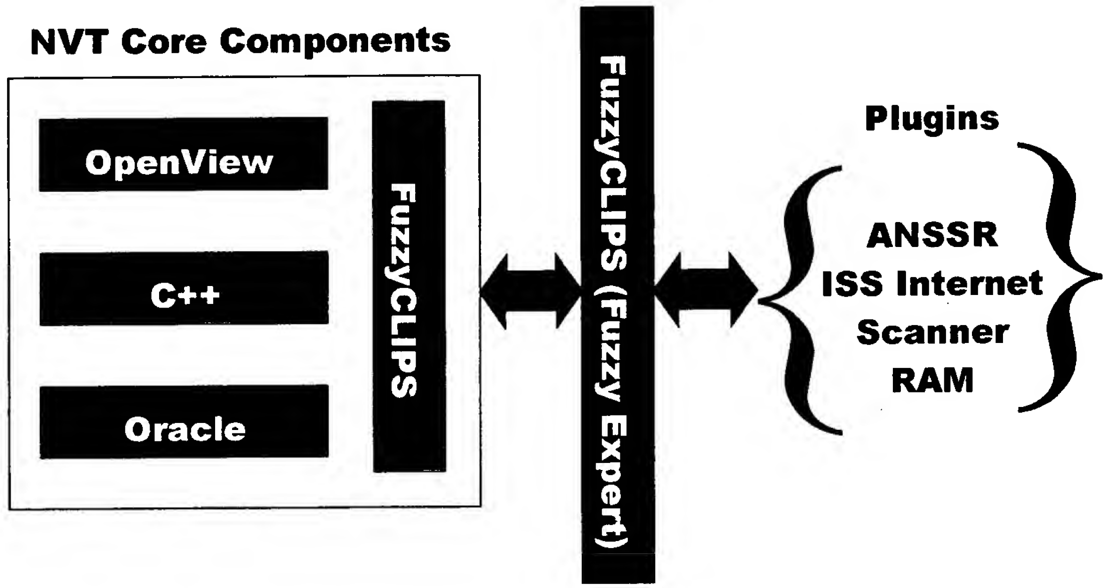
Proof-of-Concept Prototype

NVT Architecture Concept

HARRIS Electronic Systems

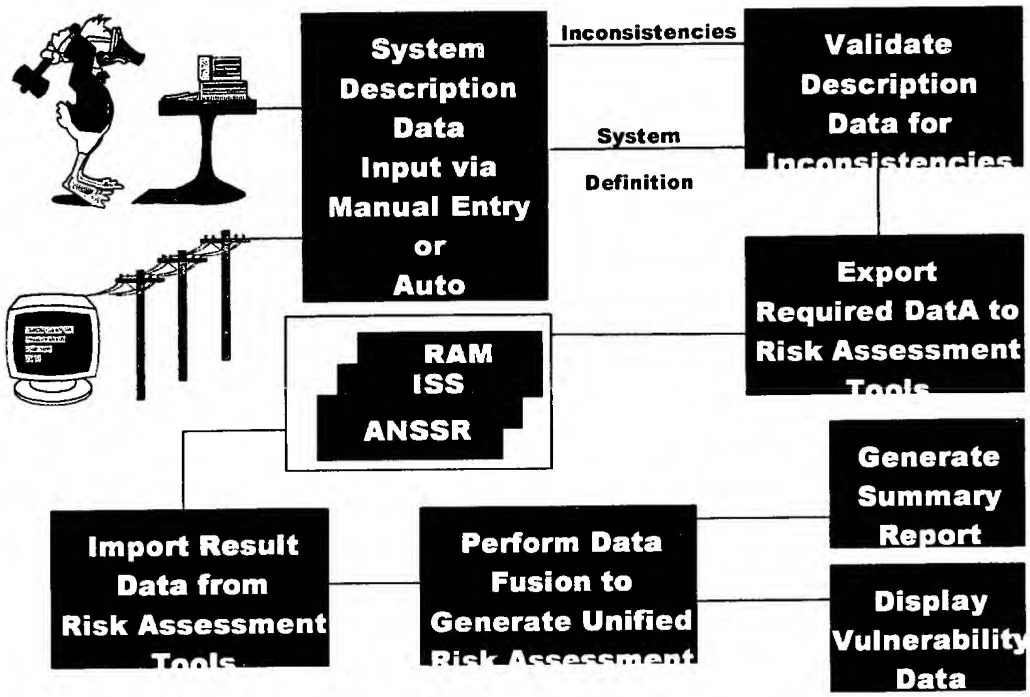


Prototype GOTS/COTS



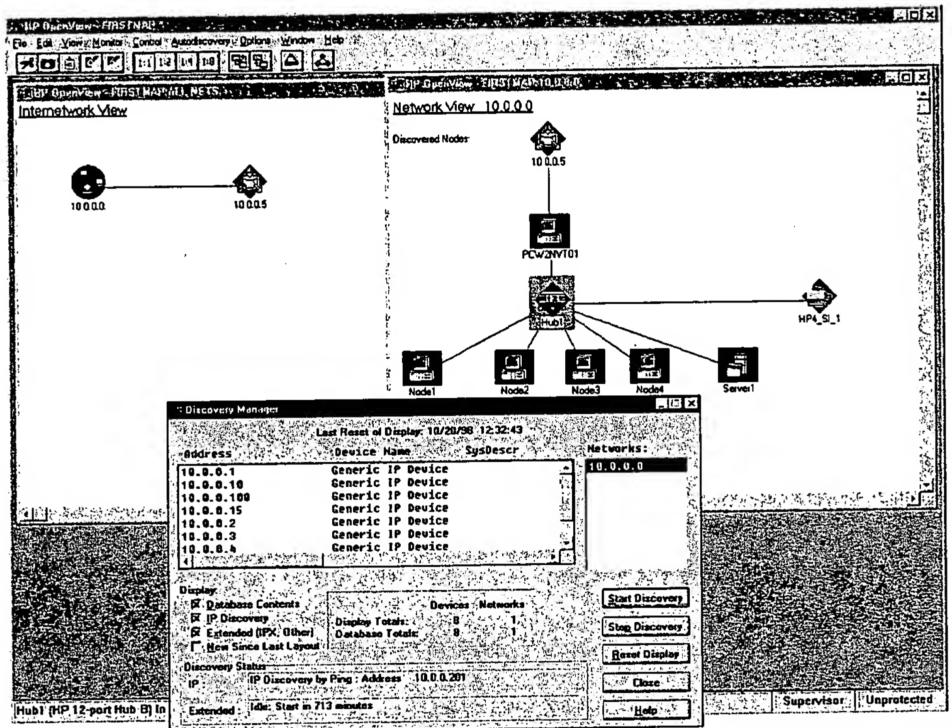
Analysis Flow Diagram

HARRIS
Electronic Systems



Automatic Discovery

HARRIS
Electronic Systems

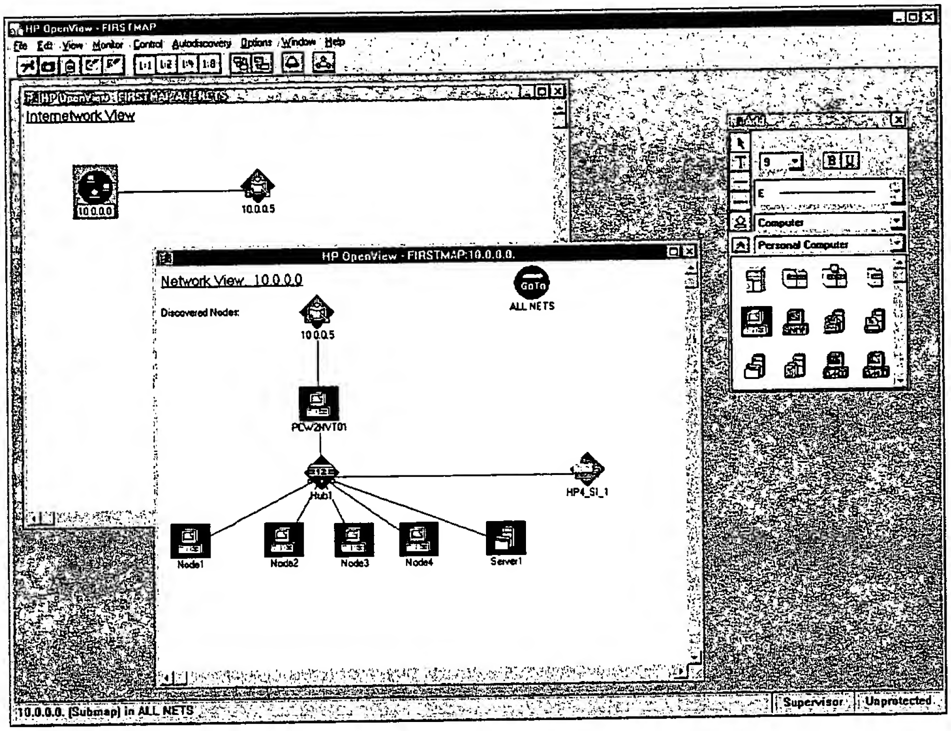


Automatic Discovery

HARRIS
Electronic Systems

- Given the IP address of the default router for the network, HP OpenView can search for computers and other devices attached to the network
- OpenView performs an active search, pinging possible IP addresses on the network
  - *Adds whatever response information it receives to its network map*

Manual Network Diagram



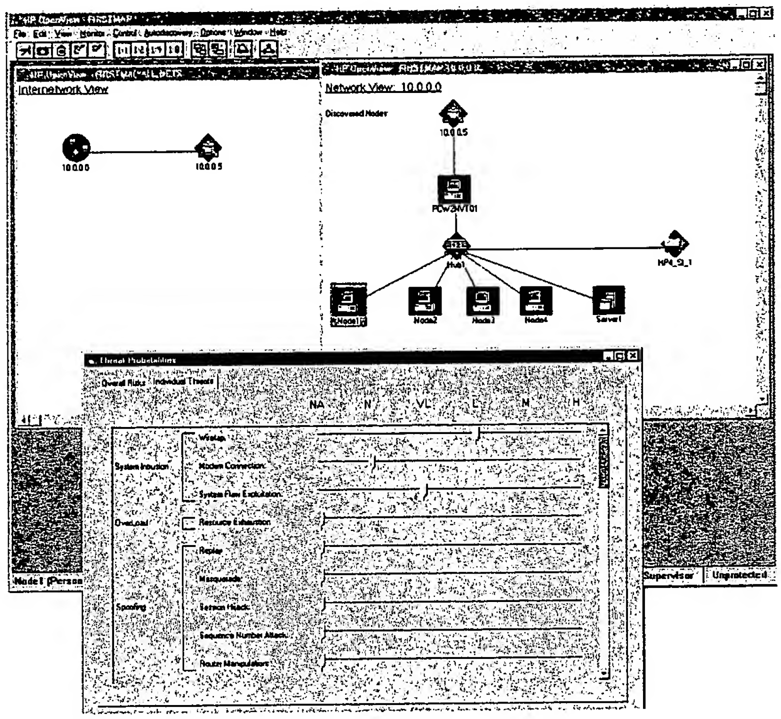
Manual Network Diagram

HARRIS Electronic Systems

- Provides a method to draw a proposed network with a graphical user interface supporting drag-and-drop
- Properties of each network node can be edited
  - *Add details as required to provide complete logical network planning*
- Can represent an entire network on a map by using a subnetwork icon
  - *Detailed map of the subnetwork can be linked to this icon and be displayed by double-clicking the subnetwork icon*

Network Node Evaluation

HARRIS
Electronic Systems



Network Node Evaluation

HARRIS Electronic Systems

- Show attack probabilities and vulnerabilities for any node on a network, even a subnetwork
- Provide methods for the user to describe the types of attacks and security risks that are of concern
- Allow user to fine-tune this information for various nodes on the network as well as establish a default value for the network
  - *This fine-tuning provides a greater level of detail for FuzzyCLIPS to provide a more accurate summary of the risk assessment*

HARRIS
Electronic Systems

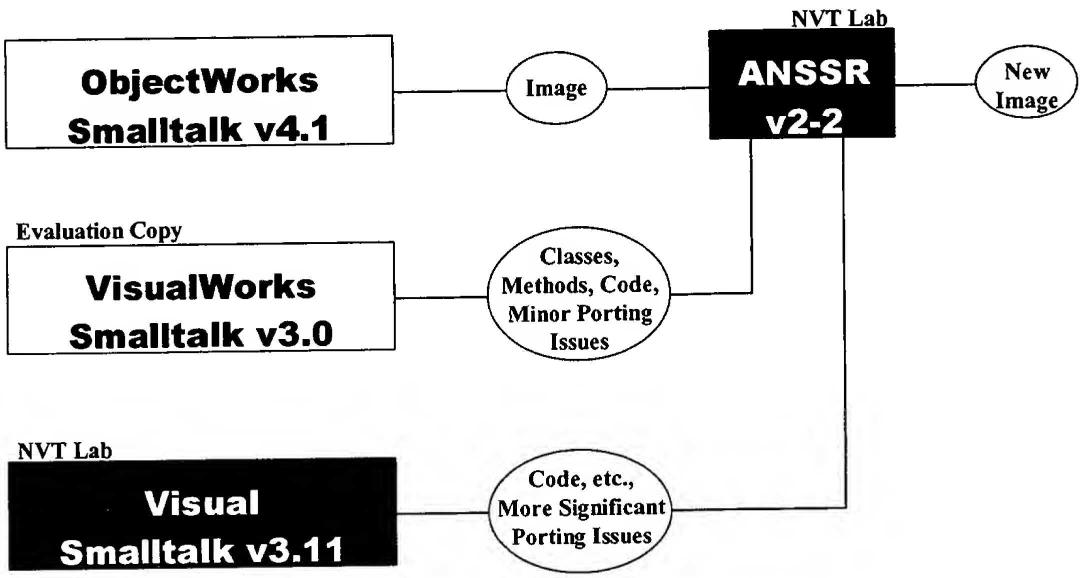
Proof-of-Concept Prototype

Risk Assessment Tools

- **Procured and installed in NVT Lab**
  - *Written in ObjectWorks Smalltalk version 4.1*
    - Encountered challenges in integrating this tool under Visual Smalltalk due to Smalltalk compatibility issues
    - Solved most compatibility issues by using VisualWorks Smalltalk, a readily available successor to ObjectWorks
      - *ANSSR has now been successfully built under VisualWorks 3.0*
    - Testing is ongoing, but outlook for use of ANSSR under VisualWorks 3.0 is promising

ANSSR Integration Issues

HARRIS Electronic Systems



ISS Internet Scanner

HARRIS Electronic Systems

- Purchased, installed in NVT Lab, and tested on the test network
- No major problems associated with integration and use in NVT are anticipated at this time

RAM

HARRIS Electronic Systems

- **Developed by NSA (R52/P5)**
  - *IO Modeling and Simulation Group*
  - *Probabilistic Fault Tree Analysis Language*
  - *Version 1.0 -- Excel Spreadsheet with 2 "helper apps"*
    - What's Best!
    - Insight
  - *Used in SABI Risk Analysis Assessment*
  - *Harris/NSA working CRADA for use of RAM in NVT*
    - Pending NSA legal review
  - *NSA also having a COTS vendor integrate it*
  - *Applied Decision Analysis (ADA) building it into DPL*
  - *Beta due out sometime in December*

RAM

HARRIS Electronic Systems

- **Recommend we use the Excel Version**
  - –*Stable*
  - –*Good experience base at NSA*
  - –*Eliminates procurement lead time*
    - •Nobody at ADA has a price for the product
  - –*Unclear if/when training will be offered*
  - –*Future maintainability of product is in question*
    - •Expected, but unsure of release cycle
    - •Unsure of maintenance costs
  - –*RAM the spreadsheet is recognizable*

Future

Risk/Vulnerability Visualization

3D Visualization

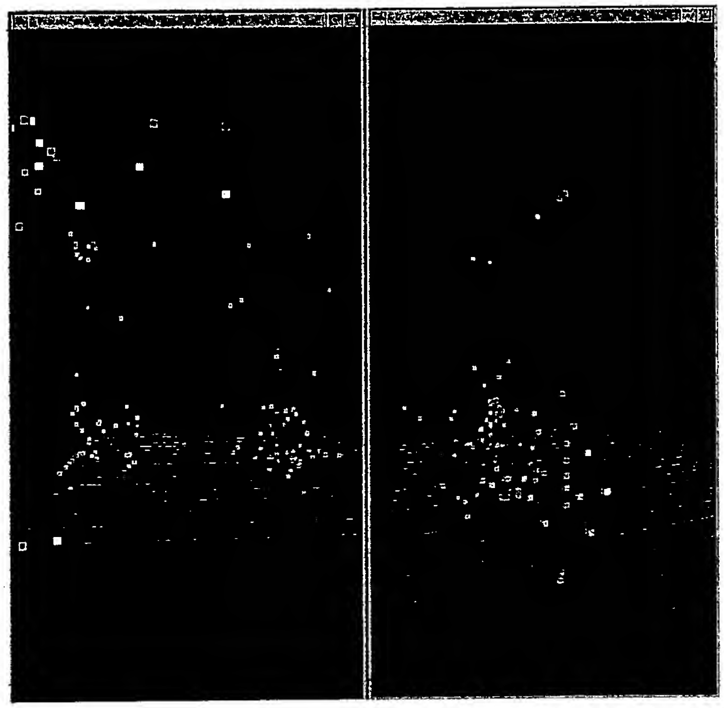
HARRIS Electronic Systems

- **VisualEyes**
  - *SGI Platform*
  - *View 3-D and n-D data sets*
  - *Information Retrieval application*
  - *Open platform*

- **Risk/Vulnerability Trade-off Analysis**
  - *A system architecture is assigned values for security, functionality, performance, availability and survivability*
  - *Display similar to text retrieval*
    - Cube represents a particular architecture design
    - Two 3D views displayed simultaneously
      - *Security, functionality and performance*
      - *Security, availability and survivability*

VisualEyes Display

HARRIS Electronic Systems



Plans for Next Quarter

Plans for Next Quarter

HARRIS Electronic Systems

- Acquire/Study Vulnerability Assessment Tools
  - *Resolve issues with ANSSR*
  - *Study ISS Internet Scanner*
  - *Get CRADA completed and Acquire RAM*
- Design Initial Prototype
- Decide Test Scenario/System
- Acquire Basic System Information (for Demo Target)
- Complete Graphical User Interface (GUI)
- Develop Fuzzy Knowledge Expert for 3 Tools

Open Discussion

Issues / Notes

Action Items

HARRIS
Electronic Systems

- **Open Action Items**
  - *–RLAI #4: AFIWC to work through Dwayne Allain to provide access to their vulnerability/risk assessment tools*
  - *–RLAI #5: Dwayne Allain to investigate providing the Air Tasking Mission Planning video*
- **New Action Items**

Backup Material

Fuzzy Technology

Fuzzy Technologies

HARRIS
Electronic Systems

- **Within fuzzy technology, several different areas were examined**
  - *–Fuzzy SQL*
  - *–Knowledge Mining*
  - *–Fuzzy Cognitive Maps*
  - *–Fuzzy Expert Technology*
- **We will touch on each area and define its applicability to our problem**

Fuzzy SQL

HARRIS Electronic Systems

- **Helps solve one problem with traditional database queries, the inability to precisely define the query**
  - *–Basis of a relational database is the establishment of a variety of independently created and maintained tables*
  - *–Tables are a set of rows and columns that are defined by a schema*
  - *–Problem with the database is that depending on the query I may get many elements, or none*
  - *–In either case, I do not get a clear understanding of how many possible answers existed or how well the returned answers fit my query*

Fuzzy SQL

- A fuzzy SQL query resolves this by understanding to what extent each possible answer "fits" (in fuzzy terms, has membership in) the solution space
- While fuzzy SQL helps resolve some issues of ambiguity for us, we have a high degree of coupling between the fuzzy rules and the database schema(s)
- This coupling may not facilitate an extensible framework, a critical design criteria
  - *We also would lack control over the rule representations because of the high dependency on SQL*

Knowledge Mining

HARRIS Electronic Systems

- Knowledge mining is the establishment of a fuzzy system that generates its own rules based on a given set of data
- Such knowledge mining applications are usually built from a variety of technologies including neural networks and genetic algorithms
- When considering knowledge mining we evaluated the many drawbacks of such a system and how they would effect our long term goals

Knowledge Mining

HARRIS Electronic Systems

- •Knowledge mining systems suffer from the following drawbacks:
  - –*Lack of meaning to rules because they were system generated*
  - –*No explanation as to how the rules were defined*
  - –*Requires a large pool of information*
  - –*Combinatorial increases in computational power requirements if not carefully managed*
- •For these reasons, it did not seem feasible to rely on this technology to provide our foundation
- •In addition, knowledge mining is more applicable to problems that have a mathematical basis, where the derived rule sets can be expressed as complex equations

Fuzzy Cognitive Maps

HARRIS Electronic Systems

- •Fuzzy Cognitive Maps were considered as a method to establish tool causal flow within our system
- •FCM's are directed cognitive maps with nodes that would identify concepts (Tools) and the edges indicate the degree to which one tool would cause or depend upon another tool
- •This technology provides a powerful capability to represent complex relationships

Fuzzy Cognitive Maps

HARRIS Electronic Systems

- The usefulness of the capability is diminished, however, because of the following limitations that have become known:
  - *FCM's represent causal relationships between concepts, but are decoupled from the actual data*
  - *Complex time relationships cannot be represented well*
  - *As the system needs to run to steadystate connectivity density, the FCM grows exponentially based on the number of concepts*
- For these reasons, this particular technology did not seem applicable to our problem
- The general consensus is that for any problem that can be solved by FCM's, fuzzy expert systems would provide a better solution